

Abstract

Verifying a cast ballot stored in a server. Forming a digital signature of the cast ballot using a private key of the server. Associating the cast ballot and the digital signature of the cast ballot using a private key of the server with a vote serial number. Forming a confirmation token, comprising the digital signature of the cast ballot using a private key of the server and the vote serial number. Making the token available to a user. Receiving a confirmation token made available to a user. Extracting a vote serial number and a digital signature of the cast ballot using a private key of the server) from the received token. For the vote serial number equal to extracted vote serial number, comparing the digital signature of the cast ballot using a private key of the server with at least one of digital signature of the cast ballot using a private key of the server and digital signature of the cast ballot using a public key of the server.